
SECURITY MANAGEMENT

Develop operational security plans

| | |
|------------------------------|--|
| level: | 6 |
| credit: | 20 |
| planned review date: | March 2007 |
| sub-field: | Security |
| purpose: | <p>This unit standard is for people who develop, or intend to develop, operational security plans.</p> <p>People credited with this unit standard are able to:</p> <ul style="list-style-type: none">- establish operational security objectives;- identify and assess operational parameters;- formulate operational security plans;- document and present operational security plans. |
| entry information: | Open. |
| accreditation option: | Evaluation of documentation and visit by NZQA, industry and teaching professional in the same field from another provider. |
| moderation option: | A centrally established and directed national moderation system has been set up by the ElectroTechnology Industry Training Organisation. |
| special notes: | <ol style="list-style-type: none">1 Legislation relevant to this unit standard includes: Building Act 1991; Companies Act 1991; Employment Relations Act 2000; Fire Service Act 1975; Health and Safety in Employment Act 1992; Privacy Act 1993; Private Investigators and Security Guards Act 1974; Resource Management Act 1991. For assessment in countries other than New Zealand, the equivalent legislation in force in that country may be used.2 Definitions <i>Analysis</i> - the systematic examination and organisation of information. |

SECURITY MANAGEMENT

Develop operational security plans

Best practice - an approved current method or way of doing something that, in the circumstances, achieves the required outcome.

Client - the person(s), or entity who contracts the task.

Duty of care - the legal and professional responsibility of a person or organisation to take due and proper care in their work.

Evaluation - the examination and comparison of information against accepted or required standards and/or other criteria to determine its value and relevance.

Operational security plan - a statement of strategies, actions and measures to achieve a desired outcome.

Procedure - a way of acting or progressing, especially an established method.

Risk - the chance of something happening that will have an impact upon objectives, measured in terms of consequences and likelihood.

Security - the protection of people, activities, and assets including information, from loss, damage, or harm.

Security industry - persons, enterprises, organisations, and other entities that provide security and security-related products and services.

Target - in terms of security, targets are people and their activities, physical and intellectual property, information, and functions, processes and systems that are the focus of inimical interest.

- 3 Range:
- a competence must be demonstrated for actual situations.
 - b evidence of two fully documented operational security plans is required.

SECURITY MANAGEMENT

Develop operational security plans

Elements and Performance Criteria

element 1

Establish operational security objectives.

performance criteria

- 1.1 Objectives are identified and are consistent with the strategic intent of the organisation and/or client.
- 1.2 Objectives are expressed in measurable terms.

element 2

Identify and assess operational parameters.

Range: typical parameters may be:
infrastructure;
personnel - skills, knowledge, availability, training, number, location;
equipment - capability, availability, reliability, contingencies;
finance - cost benefit analysis;
time - milestones, timelines, holidays;
environment - legislation, regulations, standards, culture;
commercial - contracts, market situation.

performance criteria

- 2.1 Operational parameters likely to influence operational objectives are identified.
- 2.2 Operational parameters are assessed in terms of their influence on the achievement of the operational objectives.

element 3

Formulate operational security plans.

performance criteria

- 3.1 Plans demonstrate the application and integration of relevant security concepts, techniques and technology in accordance with best practice.

SECURITY MANAGEMENT

Develop operational security plans

- 3.2 Personnel requirements, responsibilities, and performance targets are identified.
- 3.3 Equipment requirements and performance targets are identified.
- 3.4 Plans meet identified financial constraints.
- 3.5 Operational risks and costs are specified and assessed.
- 3.6 Plans include timelines, milestones, and critical dates and/or times.
- 3.7 Plans make specific provision for implementation procedures, contingency plans, coordination, monitoring, and improvement processes.
- 3.8 Plans are delivered within agreed timeframes in consultation with stakeholders.
- 3.9 Plans comply with legislative and regulatory requirements.

element 4

Document and present operational security plans.

performance criteria

- 4.1 Documentation and presentation are appropriate to the nature of the project and meet client expectations.

Range: documentation and presentation - evidence of care in presentation; substance, credibility, and clarity are not compromised by deficient spelling, punctuation or grammar; the meaning of technical terms is clear to recipients or is explained; client expectations may include - timeliness, content, clarity, conciseness, complexity, level, medium.

- 4.2 Content meets professional standards.

Range: standards include - content is structured in a logical and coherent sequence;
there are no substantive omissions or errors of fact;
assumptions, comment, inferences, conclusions and recommendations are distinguished from fact;
conclusions and recommendations are unbiased; conclusions and recommendations are consistent with the brief or objectives, facts, analysis, and evaluation;

SECURITY MANAGEMENT

Develop operational security plans

relevant legal and regulatory requirements are satisfied.

- 4.3 Measures to ensure the security of the documentation and presentation are consistent with their content and client needs.

Comments on this unit standard

Please contact the ElectroTechnology Industry Training Organisation marilyn@etito.co.nz if you wish to suggest changes to the content of this unit standard.

Please Note

Providers must be accredited by the Qualifications Authority or a delegated inter-institutional body before they can register credits from assessment against unit standards or deliver courses of study leading to that assessment.

Industry Training Organisations must be accredited by the Qualifications Authority before they can register credits from assessment against unit standards.

Accredited providers and Industry Training Organisations assessing against unit standards must engage with the moderation system that applies to those standards.

Accreditation requirements and an outline of the moderation system that applies to this standard are outlined in the Accreditation and Moderation Action Plan (AMAP). The AMAP also includes useful information about special requirements for providers wishing to develop education and training programmes, such as minimum qualifications for tutors and assessors, and special resource requirements.

This unit standard is covered by AMAP 0003 which can be accessed at <http://www.nzqa.govt.nz/framework/search/index.do>.